stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE
(DEPARTMENT OF PURE MATHEMATICS)

ZW 104/77 NOVEMBER

A.E. BROUWER

STEINER TRIPLE SYSTEMS WITHOUT FORBIDDEN SUBCONFIGURATIONS

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 05B05, 05B30

Steiner triple systems without forbidden subconfigurations

by

A.E. Brouwer

ABSTRACT

Erdős asked whether it is true that for any r there is a $v_0(r)$ such that for $v > v_0(r)$, $v \equiv 1$ or 3 (mod 6) there exists a Steiner triple system on v points such that for $2 \leq j \leq r$ no j+2 points carry j triples. [Surely this must be true.]

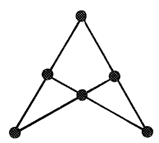
In this note we attack the first nontrivial case ($r = 4$) and prove that whenever $v \equiv 3$ (mod 6) there exists an STS(v) without four triples on six points. For $v = 7$ or 13 such an STS(v) does not exist, and we conjecture that $v_0(4) = 13$, supporting this conjecture with a few infinite series for $v \equiv 1$ (mod 6), including $v = 19$. We also give some results for $r = 5$.

KEY WORDS & PHRASES: *Steiner triple system*

0. INTRODUCTION

In [1] Erdős asked whether it is true that for any integer r there is a $v_0(r)$ such that for $v > v_0(r)$ and $v \equiv 1$ or 3 (mod 6) there exists a Steiner triple system on v points such that for $2 \le j \le r$ no j+2 points carry j triples. Note that this result would be best possible, since j+3 points always carry j triples. I conjecture that it is true, i.e. $v_0(r) < \infty$ for all r, but am not able to prove this. Probably the correct way is using a counting argument, proving that almost all of the STS(v) in a certain suitably chosen family have the desired property. In [1] Erdős remarked that Doyen had an infinite family of examples for the case r = 4. Here I solve the case r = 4, $v \equiv 3$ (mod 6) completely, and give infinitely many examples with r = 4, $v \equiv 1$ (mod 6). The methods used are mostly direct constructions, since it is usually difficult to see what happens with recursive constructions.

0A. <u>REMARK</u>. Note that there is only one configuration of 4 triples on 6 points (without repeated edges) namely {0,1,2},{0,1',2'},{1,2',0'},{1',2,0'}. I shall call it an *arrow*.

Picture: 

It is the Fano plane minus one point and the three lines incident with this point. Hence avoiding this configuration means in particular avoiding Fano subplanes. Given a Steiner triple system containing an arrow

{a,b,c},{a,d,e},{b,d,f},{c,e,f}

we can derive another Steiner triple system by replacing these four triples by the following four triples:

{a,b,d},{a,c,e},{b,c,f},{d,e,f}.

This operation is called 'inverting' the arrow.

1. CYCLIC STEINER TRIPLE SYSTEMS STS(q), $q = 6t+1$

Let q be a prime power, $q \equiv 1 \pmod 6$, $t = \frac{q-1}{6}$. A well known construction for an STS(q) is as follows: let x be a primitive element of GF(q) and take the triples $\{x^{\alpha}+i,\ x^{\alpha+2t}+i,\ x^{\alpha+4t}+i\}$ for $i \in GF(q)$ and $0 \le \alpha \le t-1$.

More generally, writing $y = x^{2t}$ so that $y^2+y+1 = 0$, we find that the collection of triples

$$\{c\{1,y,y^2\}+i \mid c \in C,\ i \in GF(q)\}$$

(where of course $c\{1,y,y^2\}+i$ means $\{c+i,\ cy+i,\ cy^2+i\}$) is a Steiner triple system iff $|C| = t$, $0 \notin C$ and if $x^{\alpha}, x^{\beta} \in C$ then $\alpha \not\equiv \beta \pmod t$.

Now let us investigate whether this system contains 4 triples on 6 points.

<u>LEMMA</u>. *Let (G,S) be an arbitrary Steiner triple system on an Abelian group G, and invariant under the natural action of G. If S contains both T and 2T and $|3T| = 3$ then S contains 4 triples on 6 points.*

<u>PROOF</u>. Let $T = \{a,b,c\}$, then $T + (a-b) = \{2a-b,a,a-b+c\}$, $T + (c-b) = \{a-b+c,c,2c-b\}$ and $2T - b = \{2a-b,b,2c-b\}$. □

(<u>REMARK</u>. A cyclic STS(15) will contain the triples $\{i,5+i,10+i\}$ and $2\{0,5,10\} = \{0,10,5\} = \{0,5,10\}$; in such a case (i.e. $b-a = c-b = a-c$; $3(b-a) = 0$) the four triples used in the proof all coincide. This explains the requirement $|3T| = 3$).

An immediate corollary is:

<u>LEMMA</u>. *The cyclic* STS(13) *contains an arrow.*

<u>PROOF</u>. It is defined by $\{1,3,9\}$ and $2\{1,3,9\} \pmod{13}$. □

As is well known there exist only two nonisomorphic STSs on 13 points. If we invert an arrow in the cyclic STS(13) we find the other STS(13), so also the other STS(13) contains an arrow.

Returning to the above construction, since $y\{1,y,y^2\} = \{1,y,y^2\}$, the only actual freedom we have is choosing c from $\{c,-c\}$ (note that $-1 = x^{3t}$). Now once we have chosen c we cannot choose 2c and therefore must choose $-2c$, i.e.: If an STS(q) constructed as abvoe does not contain arrows then it is invariant under multiplication by -2.

In particular, since there are only qt triples, the order of -2 is a divisor of t, i.e. -2 is a square in GF(q) and for $q = p^\alpha$, p prime it follows that either α is even or $p \equiv 1$ or 3 (mod 8).

Consider again the case of two congruent triples in an arrow:

$S_1 = \{a,b,c\}$ and $S_2 = \{2a-b,a,a-b+c\}$.

The case where $a-b+c$ and c are connected in the arrow was considered above; in the other case we have

$S_3 = \{b,a-b+c,d\}$ and $S_4 = \{2a-b,c,d\}$.

All four triples are shifts of multiples of $\{1,y,y^2\}$ so we may suppose $b = ay$, $c = ay^2$. Now $(a-b+c)-b = a(1-y)^2 = (a-b)(1-y)$ and $c - (2a-b) = -3a = (c-a)(1-y)$ so that S_3 and S_4 are both shifts of $\pm(1-y)S_1$. In particular S_3 and S_4 are congruent themselves and by the same reasoning it follows that S_1 and S_2 are shifts of $\pm(1-y)^2S_1 = \pm(-3y)S_1 = \pm(-3)S_1$. But if S_1 is a shift of $\pm 3S_1$ then $y = \pm 3$ (or $y^2 = \pm 3$), $1 = y^3 = \pm 27$, $p = 7$ or 13.

Conversely, if $p = 7$ then $y = 2$, and already the shifts by elements of GF(7) of $\{1,2,4\}$ (or of $-\{1,2,4\}$) form a Fano subplane of our Steiner triple system. Furthermore, if $p = 13$ then $y = 3$, and the shifts of $\pm\{1,3,9\}$ and $\pm\{2,6,5\}$ form a sub STS(13). (Generally of course if $p \equiv 1$ (mod 6) then we have a sub STS(p)).

Finally consider an arbitrary arrow. By normalizing if necessary we may assume it contains $S_1 = \{1,y,y^2\}$. If $1 \in S_2$ and S_2 is a shift of cS_1 then w.l.o.g. $S_2 = \{1,1-c+yc,1-c+y^2c\}$, but $1-c+yc-y = (c-1)(y-1)$ and $1-c+y^2c-y^2 = (c-1)(y^2-1)$ hence if $S_3 = \{y,1-c+yc,z\}$, $S_4 = \{y^2,1-c+y^2c,z\}$ then both S_3 and S_4 are shifts of $\pm(c-1)S_1$ so that they are congruent, and we are in the previous case.

Therefore $S_3 = \{y^2, 1-c+yc, z\}$, $S_4 = \{y, 1-c+y^2c, z\}$.
From S_3 we find either $z - (1-c+yc) = y(1-c+yc-y^2)$, i.e. $z = y(1-c)-2c$
or $1-c+yc-y^2 = y(z-(1-c+yc))$, i.e. $z = 2y(c-1)+c$.
From S_4 we find either $z - (1-c+y^2c) = y(1-c+y^2c-y)$, i.e. $z = -2y(c-1)c+2$
or $1-c+y^2c-y = y(z-(1-c+y^2c))$, i.e. $z = y(c-1)-c-1$.
But these values of z are not compatible:

From $y(1-c)-2c = y(c-1)-c-1$ or $2y(c-1)+c = -2y(c-1)-c+2$ we find $y = -\frac{1}{2}$ or $c = 1$, but $y^3 = -\frac{1}{8} = 1$ is impossible since $q \equiv 1 \pmod 6$, so that $c = 1$.

From $y(1-c)-2c = -2y(c-1)-c+2$ we find $c = y^2$, and from $2y(c-1)+c = y(c-1)-c-1$ we find $c = y$.
In all cases $c \in \{1, y, y^2\}$ so that S_2 is a shift of S_1.

Thus we have shown:

THEOREM 1. *Let* $q \equiv 1 \pmod 6$, $q = p^\alpha$, p *prime and construct a Steiner triple system* S_C *as above.*

(i) *If* $p = 7$ *or* 13 *then* S_C *contains a* sub-STS(p), *and in particular an arrow.*

(ii) *If* $p \neq 7, 13$ *then* S_C *contains an arrow iff for some* $S \in S_C$ *also* $2S \in S_C$, *where* $S \neq 2S$.

Hence C *can be chosen such that* S_C *does not contain an arrow iff* -2 *is a square, i.e. iff* $\alpha \equiv 0 \pmod 2$ *or* $p \equiv 1$ *or* $3 \pmod 8$. *Any arrow contains three edges which are translates of each other.* □

Later we shall need the next:

LEMMA. *There exists an* STS(21) *with a parallel class and without arrow.*

PROOF. The cyclic STS(21) defined by

{0,1,3},{0,4,12},{0,6,11},{0,7,14} mod 21

contains the parallel class [{0,7,14} mod 21]. Checking that it does not contain an arrow is left to the reader. □

2. THE CASE $v \equiv 3 \pmod 6$

In this section we prove

THEOREM 2. *Let* $v \equiv 3 \pmod 6$. *Then there exists an* STS(v) *without arrows.*

Let $v = 3q$, q odd (not necessarily a prime power). Let $(Q,\circ)$ be an idempotent commutative quasigroup on Q, where $|Q| = q$. (One might for example take $Q = \mathbb{Z}_q$ and $a\circ b = \frac{a+b}{2}$.) As is well known one obtains an STS(v) on $X = Q \times \mathbb{Z}_3$ by taking the triples $\{q\} \times \mathbb{Z}_3$ for $q \in Q$ (note that these form a parallel class) and

$$\{(a,i),(b,i),(a\circ b,i+1)\} \quad \text{for } a,\ b \in Q,\ i \in \mathbb{Z}_3.$$

It is easily checked that this Steiner triple system contains an arrow iff

(i) $\exists a,b \in Q,\ a \neq b$: $a\circ(a\circ(a\circ b)) = b$

[An arrow is given by $\{\{a\} \times \mathbb{Z}_3,\ \{(a,0),(b,0),(a\circ b,1)\},$ $\{(a,1),(a\circ b,1),(a\circ(a\circ b),2)\},\ \{(a,2),(a\circ(a\circ b),2),(b,0)\}\}$.]

or

(ii) $\exists a,b,c,d \in Q$, all distinct: $a\circ b = c\circ d$ and $a\circ c = b\circ d$

[that is, the Latin square that is the multiplication table of $(Q,\circ)$ contains a 2×2 subsquare. In this case an arrow is given by $\{\{(a,0),(b,0),(a\circ b,1)\},\{(c,0),(d,0),(c\circ d,1)\},$ $\{(a,0),(c,0),(a\circ c,1)\},\{(b,0),(d,0),(b\circ d,1)\}\}$.].

Now let $(Q,\circ)$ be the example indicated above: $(\mathbb{Z}_q, \frac{\cdot+\cdot}{2})$. We have $a\circ(a\circ(a\circ b)) = \frac{7}{8}a + \frac{1}{8}b$ so that $a\circ(a\circ(a\circ b)) = b$ iff $7(a-b) = 0$. also $\frac{a+b}{2} = \frac{c+d}{2}$ and $\frac{a+c}{2} = \frac{b+d}{2}$ implies $a = d$, $b = c$.
This proves

LEMMA. *The* STS(v) *constructed from* $(\mathbb{Z}_q, \frac{\cdot+\cdot}{2})$ *as above contains an arrow iff* $7|q$.

In order to prove theorem 2 we have to find an STS(v) without arrows for $21|v$. For $v = 21$ this has been done in §1.

[After trying all posibilities I found that there is no commutative idempotent quasigroup of order 7 such that the associated Steiner triple system of order 21 is free from arrows. Consequently the direct construction given in §1 is indispensable.]

For $v > 21$ we use a recursive construction:
Let $v = 7u$, $u \equiv 3 \pmod 6$ and let S be an STS(u) on a set U with a parallel class P and without arrow. We construct an STS(v) with parallel class and without arrow as follows:

Let $V = I_7 \times U$ and take the following triples:

(i) for each $T \in S \backslash P$ take the triples of a transversal design $T[3,1;7]$ on $I_7 \times T$ with groups $I_7 \times \{t\}$ $(t \in T)$, where this transversal design (Latin square of order 7) does not contain an arrow (Latin subsquare of order 2); a suitable Latin square is for example the addition table of $\mathbb{Z}_7$.

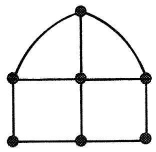
(ii) for each $T \in P$ take the triples of an STS(21) with parallel class P_T and without arrows on $I_7 \times T$.

Obviously this yields an STS(v) with parallel class $\bigcup_{T \in P} P_T$. If it contains an arrow, and all four triples are of type (i) then projecting them down yields an arrow in S unless two triples have the same projection T. But in this case all four have the same projection, and we have an arrow in the transversal design on $I_7 \times T$. Contradiction. If two triples are of type (ii) then (since they intersect) they have the same projection T and it follows that all four are in the STS(21) on $I_7 \times T$. Contradiction. Finally with three triples of type (i) and one of type (ii) we find a contradiction if two have the same projection T, hence the three triples of type (i) project in three intersecting triples so that the triple of type (ii) has to project into a triple too and again we found an arrow at the bottom (i.e. in S). This proves that our STS(v) is free of arrows, which completes the proof of theorem 2.

3. THE CASE $r = 5$

It is easy to verify that the only configuration of five triples on seven points not containing an arrow is given by

{0,1,1'},{0,2,2'},{0,3,3'},{1,2,3},{1',2',3'}.
I shall call it a *mitre*.

Picture: 

It is the affine plane AG(2,3) minus two points and the seven lines incident with these points. Hence avoiding this configuration means in particular also avoiding sub STS(q)'s.

Let us now investigate for which quasigroups $(Q,\circ)$ the associated Steiner triple system S_Q contains a mitre. If the two disjoint triples are embedded vertically, we find the mitre

$\{\mathbb{Z}_3\times\{a\},\mathbb{Z}_3\times\{b\},\{(0,c),(0,a),(1,b)\},$
$\{(0,c),(0,b),(1,a)\},\{(0,c),(2,a),(2,b)\}\}$

and it follows that {a,b,c} is a quasigroup of order 3:

$a\circ b = c,\ a\circ c = b,\ b\circ c = a.$

If there is one vertical triple we find the mitre

$\{\mathbb{Z}_3\times\{a\},\{(1,a),(1,b),(2,a\circ b)\},\{(2,a),(2,d),(0,a\circ d)\},$
$\{(0,a),(1,b),(0,a\circ d)\},\{(0,a),(2,a\circ b),(2,d)\}\}$

and it follows that $a = d\circ(a\circ(a\circ(a\circ d)))$. All other cases lead to a contradiction, so we have

<u>LEMMA</u>. *S_Q contains a mitre iff* Q *contains distinct elements* a, b *such that*

$$a = b\circ(a\circ(a\circ(a\circ b))). \qquad (1)$$

(Note that (1) holds in case {a,b,c} is a subquasigroup of Q).

If we take the special quasigroup $(Q_0,\circ) = (Z_q, \frac{\cdot+\cdot}{2})$ then (1) holds iff $9(a-b) = 0$, so that $3|q$.
Hence

<u>THEOREM</u>. *Let* $(q,42) = 1$ *and* $v = 3q$. *Then there exists an* STS(v) *without arrow or mitre, sc.* S_{Q_0}.

REFERENCE

[1] ERDÖS, PÁL, *Problems and results in comb. analysis*, Creation in Mathematics no.9 (1976) p.25.

Tel Aviv, oct. 1977

MC, 771125